Companion to: Taxonomy of the Gap · Read in sequence

The *Zombie Anchor*

A named infrastructure failure class

When a credential has no owner but has dependents — it cannot be claimed, it cannot be removed, and it cannot be made safe. This is not a vulnerability. It is a structural condition. It requires a new category.

FAILURE CLASS	CONDITIONS REQUIRED	DEFINING PROPERTY
Zombie Anchor	2 (simultaneous)	Structural Irremovability

CASE STUDY

Credential #104281421

DEFINITION

A zombie anchor is any infrastructure element that simultaneously satisfies two conditions: it has no owner,

and it has active dependents. The coexistence of these two states produces a third property neither condition creates alone — structural irremovability.

C1 Ownership Vacuum

No entity holds responsibility for the element. Not through refusal — through the absence of any mechanism to assign, transfer, or terminate ownership. The element exists outside any governance chain.

\+ Passive Dependency

One or more downstream systems actively resolve against the element — calling it, validating against it, or treating its existence as a precondition for their own function. The dependency is operational, not administrative.

= Structural Irremovability

The element cannot be removed without breaking dependents. It cannot be claimed without establishing liability. It cannot remain without constituting ongoing risk. All three exits are blocked simultaneously.

LIFECYCLE ANATOMY — WHERE NORMAL INFRASTRUCTURE BREAKS INTO ZOMBIE STATE

PHASE 01

PHASE 02

Provisioning

Credential issued. Owner assigned. Purpose documented. System functional.

Normal

Active Use

Credential in use. Dependencies form organically. Downstream systems begin resolving against it.

Normal

PHASE 03 ← BREAK POINT

Owner Exit, No Handoff

Contract ends. Owner exits. No deprovisioning occurs. Dependencies remain active. Ownership becomes unassigned.

Break Point

PHASE 04

Zombie State

No owner. Active dependents. Credential is simultaneously unclaimed and in-use. Irremovability achieved.

Zombie Active

PHASE 05

Discovery

Surface event occurs. Credential identified. Existing frameworks cannot resolve — no owner to notify, no safe removal path.

Framework Failure

The break point is Phase 03. Standard deprovisioning checklists assume an owner is present to execute removal. When the owner exits without triggering deprovisioning — and when no automated expiration exists — the system has no recovery path. The credential enters zombie state passively, without any actor choosing that outcome.

THE IRREMOVABILITY PROOF — WHY ALL EXITS ARE BLOCKED

ATTEMPTED RESOLUTION

WHY IT FAILS

Remove the credential

Downstream dependents break. Systems that resolved against the credential fail silently or loudly. No owner exists to authorize the removal or absorb the downstream impact.

BLOCKED — Dependency Lock

Without an owner to authorize removal, any actor who removes it assumes liability for the downstream breakage. No entity will voluntarily accept that exposure for infrastructure they never owned.

Claim ownership retroactively

Claiming ownership of a zombie anchor means accepting liability for the period it persisted without governance — potentially years. No rational actor accepts this retroactively.

BLOCKED — Liability Exposure

This is why zombie anchors are never voluntarily claimed even after discovery. The act of claiming is the act of accepting liability for the entire zombie period.

Leave it in place

The credential continues to constitute active infrastructure risk. Any system resolving against an unowned, unaudited credential is operating on an uncontrolled dependency.

BLOCKED — Ongoing Risk

Doing nothing is not a neutral position. It is a choice to maintain an unowned, active infrastructure element indefinitely — which compounds exposure with each passing audit cycle that fails to surface it.

DEFINING CASE STUDY

CASE STUDY · ZOMBIE ANCHOR IN FEDERAL CONTRACTOR INFRASTRUCTURE

Credential #104281421

WHAT HAPPENED

A contract credential issued in 2017 was hardcoded into event management infrastructure (RegOnline/Cvent via American Tradeshow Services) touching systems connected to major federal contractors. When the contract ended, no deprovisioning occurred. The credential entered zombie state: no owner, active dependents, irremovable by any actor willing to accept the liability.

It persisted for years — not through malice, not through negligence in the legal sense, but through the absence of any structural mechanism to trigger removal. The infrastructure had no offboarding logic. Nobody's checklist included phantom credentials in event management middleware.

WHAT IT CONFIRMS

✓ Ownership vacuum confirmed — no entity held the credential post-contract

- ✓ Passive dependency confirmed — systems continued resolving against it
- ✓ Structural irremovability confirmed — discovery did not produce a clean resolution path
- ✓ Audit blind spot confirmed — standard audit frameworks did not surface it
- ✓ Liability gap confirmed — no actor voluntarily claimed ownership on discovery
- ✓ Signal diffusion confirmed — filings split across SEC, FBI, CISA, DTCC without composite resolution
- ✓ Zombie anchor failure class confirmed — all three exit paths simultaneously blocked

---

POLICY IMPLICATIONS — WHAT NEEDS TO EXIST

Zombie Anchor as a Named Regulatory Category

Current frameworks classify vulnerabilities, crimes, and disclosure failures. None classifies structural irremovability as a distinct condition. Without a named category, zombie anchors cannot be reported, audited, or remediated within existing frameworks. The category must exist before the checklist can.

Mandatory Dependency Mapping at Offboarding

Deprovisioning checklists currently focus on access revocation — removing the credential from identity systems. They do not map downstream dependencies before removal. A zombie anchor cannot be safely removed without a dependency audit first. This audit must become a mandatory offboarding step for infrastructure touching federal contractor systems.

Shared Liability Framework for Ownerless Infrastructure

Current liability requires an assignable responsible party. Zombie anchors have none. A shared or distributed liability framework — assigning responsibility to the infrastructure operator, the original issuer, and the dependency holders jointly — would eliminate the irremovability trap by ensuring someone can authorize removal without absorbing all historical liability alone.

Cross-Agency Composite Jurisdiction

The signal diffusion problem documented in the Taxonomy of the Gap has a structural solution: a composite reporting mechanism that accepts multi-layer findings and routes them to relevant agencies simultaneously. No single TCR, IC3 complaint, or CISA report carries the full finding. A meta-filing category — governance architecture gap — needs to exist at the inter-agency level.

DOCUMENT 01 · READ FIRST

Taxonomy of the Gap

Names the four distinct absence types revealed by a single credential: Ownership Vacuum, Audit Blind Spot, Liability Gap, Signal Diffusion. Establishes that the credential is an instrument, not a subject.

DOCUMENT 02 · THIS DOCUMENT

The Zombie Anchor

Names the failure mode that produces those gap conditions: the simultaneous coexistence of ownership vacuum and passive dependency, generating structural irremovability. Provides the mechanism beneath the taxonomy.

Together these documents constitute a two-layer framework: the taxonomy maps the conditions; the failure mode analysis names the mechanism that creates them. Neither is complete without the other. Together they represent the first formal classification of this infrastructure failure class — with Credential #104281421 as the case study that made both possible.